

Poisson distribution of a prime counting function corresponding to elliptic curves

R. Balasubramanian and Sumit Giri

ABSTRACT

Let E be an elliptic curve defined over rational field \mathbb{Q} and N be a positive integer. Now $M_E(N)$ denotes the number of primes p , such that the group $E_p(\mathbb{F}_p)$ is of order N . We show that $M_E(N)$ follows Poisson distribution when an average is taken over a large class of curves.

1. Introduction

Let E be an elliptic curve defined over the field of rationals \mathbb{Q} . For a prime p where E has good reduction, we denote by E_p the reduction of E modulo p . Let \mathbb{F}_p be the finite field with p elements and $E_p(\mathbb{F}_p)$ be the group of \mathbb{F}_p points over E_p .

We know $|E_p(\mathbb{F}_p)| = p + 1 - a_p(E)$ where $a_p(E)$ is the trace of the Frobenius morphism at p . By Hasse's theorem we know $|a_p(E)| < 2\sqrt{p}$. Also, it is well known that $E_p(\mathbb{F}_p)$ admits the structure of an abelian group of the form $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mk\mathbb{Z}$, where m divides $(p-1)$. We denote such groups by $G_{m,k}$. The question related to density of elliptic curve groups among all groups of the form $G_{m,k}$ has been addressed in [BPS12]. Also, the question related to the primality of $E_p(\mathbb{F}_p)$ has been discussed in [BCD11].

For a fixed positive integer N , we define the following prime counting function

$$M_E(N) := \#\{p \text{ prime} : E \text{ has good reduction over } p \text{ and } |E_p(\mathbb{F}_p)| = N\}. \quad (1.1)$$

Here we note that the Hasse's theorem implies

$$(\sqrt{p} - 1)^2 < N < (\sqrt{p} + 1)^2$$

or equivalently,

$$N^- := (\sqrt{N} - 1)^2 < p < (\sqrt{N} + 1)^2 := N^+. \quad (1.2)$$

This in turn implies that

$$M_E(N) \ll \frac{\sqrt{N}}{\log(N+1)}. \quad (1.3)$$

Using Chinese Remainder theorem, it is not difficult to construct a curve E such that the upper bound in (1.3) is attained.

Also, it is not difficult to prove that

$$\sum_{N \leq x} M_E(N) = \pi(x) + O(\sqrt{x}). \quad (1.4)$$

Consequently, $M_E(N)$ is zero for most of the N 's. Under the assumption that $E_p(\mathbb{F}_p)$ is uniformly distributed over the range $[p^-, p^+]$, $M_E(N)$ is expected to be $\sim \frac{c}{\log N}$. See equation (4) in [DS13] for more details.

Now, for a pair of integers (a, b) , let $E_{a,b}$ be the elliptic curve defined by the Weierstrass equation

$$E_{a,b} : y^2 = x^3 + ax + b.$$

Also for $A, B > 0$, we define the class of curves $\mathcal{C}(A, B)$ by

$$\mathcal{C}(A, B) := \{E_{a,b} : |a| \leq A, |b| \leq B, \Delta(E_{a,b}) \neq 0\}. \quad (1.5)$$

Now us recall Barban-Davenport-Halberstam conjecture

CONJECTURE 1 *BDH*. Let $\theta(x; q, a) = \sum_{p \leq x, p \equiv a \pmod{q}} \log p$. Let $0 < \eta \leq 1$ and $\beta > 0$ be real numbers. Suppose that X, Y , and Q are positive real numbers satisfying $X^\eta \leq Y \leq X$ and $Y/(\log X)^\beta \leq Q \leq Y$. Then

$$\sum_{q \leq Q} \sum_{\substack{1 \leq a \leq q \\ (a, q) = 1}} |\theta(X + Y; q, a) - \theta(X; q, a) - \frac{Y}{\phi(q)}|^2 \ll_{\eta, \beta} YQ \log X.$$

Under the above hypothesis concerning short interval distribution of primes in arithmetic progressions, David and Smith[DS13, DS14] proved that

THEOREM A. Let Conjecture 1 be true for some $0 < \eta < \frac{1}{2}$. If $A, B \geq \sqrt{N}(\log N)^{1+\gamma} \log \log N$ and that $AB \geq N^{\frac{3}{2}}(\log N)^{2+\gamma} \log \log N$, then for any odd integer N , we have

$$\frac{1}{\#\mathcal{C}(A, B)} \sum_{E \in \mathcal{C}(A, B)} M_E(N) = K(N) \frac{N}{\phi(N) \log N} + O\left(\frac{1}{(\log N)^{1+\gamma}}\right), \quad (1.6)$$

with

$$K(N) := \prod_{p \nmid N} \left(1 - \frac{(\frac{N-1}{p})^2 p + 1}{(p-1)^2(p+1)}\right) \prod_{p \mid N} \left(1 - \frac{1}{p^{\nu_p(N)}(p-1)}\right), \quad (1.7)$$

where ν_p denotes the usual p -adic valuation where $\nu_p(n)$ and $\left(\frac{n-1}{p}\right)$ is the Kronecker symbol.

In [CDKS15], Chandee, David, Koukoulopoulos and Smith extended this result over all N .

From [Theorem 1.7, [CDKS15]], unconditionally, we also have

$$\frac{1}{\#\mathcal{C}(A, B)} \sum_{E \in \mathcal{C}(A, B)} M_E(N) \ll \frac{N}{\phi(N) \log N} = O\left(\frac{\log \log N}{\log N}\right) \quad (1.8)$$

for large enough A, B .

Note that the above theorem is based on the assumption of Barban-Davenport-Halberstam conjecture for a particular range. Martin, Pollack and Smith[MPS14] and authors[BG15] independently computed the mean value of $NK(N)/\phi(N)$ to show that Theorem A is consistent with (1.4).

In this paper we try to focus on the distribution of the function $M_E(N)$. In other words, if N is a fixed integer and E be any arbitrary chosen curve from a large class of curves, then what is the probability of the event $\{M_E(N) = \ell\}$ where ℓ is a positive integer.

Under the assumption that primes are randomly distributed and reduction modulo two different primes are two independent events, one would expect the event $\{E \in \mathcal{C} : M_E(N) = \ell\}$ occurs with a probability $\sim \frac{1}{(\log N)^\ell}$. The main theorem of this paper is

THEOREM 1. *Let $\mathcal{C}(A, B)$ be as defined as in (1.5) and N be a positive integer greater than 7. If L be a positive integer such that $A, B > N^{L/2}(\log N)^{1+\gamma}$ and $AB > N^{3L/2}(\log N)^{2+\gamma}$ for some $\gamma > 0$, then for $1 \leq \ell \leq L$*

$$\frac{1}{\#\mathcal{C}(A, B)} \sum_{\substack{E \in \mathcal{C}(A, B) \\ M_E(N) = \ell}} 1 = \frac{1}{\ell!} \left(\frac{1}{\#\mathcal{C}(A, B)} \sum_{E \in \mathcal{C}(A, B)} M_E(N) \right)^\ell \left(1 + O\left(\frac{N}{\phi(N) \log N} \right) \right) + O\left(\frac{1}{N^{\frac{L-\ell}{2}} (\log N)^\gamma} \right),$$

where the ‘ O ’ constant in the last error term is independent of γ .

Now we know that if $X_N \sim \text{Poisson}(\lambda_N)$, for $N = 1, 2, \dots$, then the probability mass function of X_N is

$$f_{X_N}(\ell) = \frac{(\lambda_N)^\ell e^{-\lambda_N}}{\ell!} \quad \text{for } \ell = 0, 1, 2, \dots$$

If we take $\lambda_N = \frac{1}{\#\mathcal{C}(A, B)} \sum_{E \in \mathcal{C}(A, B)} M_E(N)$, then in view of (1.8), one can see that if L is large, then on an average $M_E(N)$ follows a limiting Poisson distribution with mean $\frac{1}{\#\mathcal{C}(A, B)} \sum_{E \in \mathcal{C}(A, B)} M_E(N)$ as $N \rightarrow \infty$. The integer L in *Theorem 1* is introduced to ensure the finiteness of the class $\mathcal{C}(A, B)$.

One can immediately see that if one also assumes Conjecture 1, as in Theorem A, then the right hand side is asymptotic to $\frac{1}{\ell!} \left(\frac{NK(N)}{\phi(N) \log N} \right)^\ell$.

In [Kow06], Kowalski raised a question related to the behavior of sums of the type

$$\sum_{N \leq x} M_E(N)^r \quad \text{and} \quad \sum_{\substack{N \leq x \\ M_E(N) \geq 2}} M_E(N).$$

To answer this question, we start with the quantity

$$\frac{1}{\#\mathcal{C}} \sum_{E \in \mathcal{C}} \sum_{\substack{M_E(N) \geq \ell \\ N \leq x}} M_E(N)^r \tag{1.9}$$

for two non negative integers r and ℓ .

Before stating our result related to (1.9), we shall introduce a sequence of constants $\{C(m)\}_{m=\ell}^\infty$, where $C(m)$ corresponds to the m -th moment of the function $NK(N)/\phi(N)$ where $K(N)$ as defined in (1.7). More precisely,

$$C(m) = \prod_{p > 2} \left(1 - \frac{1}{(p-1)^2} \right)^m \prod_p (1 + f_m(p)),$$

where,

$$\begin{aligned}
 f_m(2) &= \frac{1}{2} \left(\left(\frac{2}{3} \right)^m - 1 \right) + 2^m \sum_{j \geq 2} \frac{1}{2^j} \left(\left(1 - \frac{1}{2^j} \right)^m - \left(1 - \frac{1}{2^{j-1}} \right)^m \right), \\
 f_m(p) &= \frac{1}{p} \left[\left(1 - \frac{1}{(p-1)^2} \right)^{-m} \left(\left(1 - \frac{1}{(p-1)^2(p+1)} \right)^m + \left(\frac{p}{p-1} \right)^m \left(1 - \frac{1}{p(p-1)} \right)^m \right) - 2 \right] \\
 &\quad + \left(\frac{p}{p-1} \right)^m \left(1 - \frac{1}{(p-1)^2} \right)^m \sum_{j \geq 2} \frac{1}{p^j} \left(\left(1 - \frac{1}{p^j(p-1)} \right)^m - \left(1 - \frac{1}{p^{j-1}(p-1)} \right)^m \right).
 \end{aligned} \tag{1.10}$$

It is easy to check that $C(1) = 1$. It seems difficult to simplify the expression when $m > 1$.

Also, for two integers $r \leq \ell$, we construct a sequence $\{d_{\ell,r}(m)\}_{m=\ell}^\infty$ as follows

$$d_{\ell,r}(m) = \sum_{k=\ell}^m \frac{k^r}{k!} \frac{(-1)^{m-k}}{(m-k)!} \tag{1.11}$$

Here we note that $d_{\ell,r}(\ell) = \frac{\ell^r}{\ell!}$; Also $d_{1,1}(1) = 1$ and $d_{1,1}(m) = 0$ for $m \geq 2$.

With these notations, our next theorem is as follows

THEOREM 2. *Let r and ℓ be two positive integers with $r \leq \ell$. Also suppose γ_1 be non negative integer and γ_2 is a positive real number with $1 + \gamma_1 \leq \gamma_2$. Now if $\mathcal{C}(A, B)$ be defined as in (1.5) with $A, B > x^{\frac{\ell+\gamma_1}{2}} (\log x)^{1+\ell+\gamma_2}$ and $AB > x^{\frac{3(\ell+\gamma_1)}{2}} (\log x)^{2+\ell+\gamma_2}$, then for any positive real number x ,*

$$\frac{1}{\#\mathcal{C}(A, B)} \sum_{E \in \mathcal{C}} \sum_{\substack{N \leq x \\ M_E(N) \geq \ell}} M_E(N)^r = \sum_{m=\ell}^{\ell+\gamma_1} C(m) d_{\ell,r}(m) Li_m(x) + O\left(\frac{x}{(\log x)^{1+\ell+\gamma_1}}\right),$$

where $C(m)$ and $d_{\ell,r}(m)$ are defined in (1.10) and (1.11) respectively and $Li_m(x) = \int_2^x \frac{1}{(\log t)^m} dt$.

We note that a theorem in [CDKS15], stated as Proposition 1 later in this paper enables one to prove Theorem 2 unconditionally. Further conditionally as in Theorem A, one has

THEOREM 3. *Let Conjecture 1 be true for some $\eta < 1$. Also let γ_1 be a non negative integer and $\gamma_2 > 0$. Now if $A, B > x^{\frac{\ell+\gamma_1}{2}} (\log x)^{1+\ell+\gamma_2}$ and $AB > x^{\frac{3(\ell+\gamma_1)}{2}} (\log x)^{2+\ell+\gamma_2}$, then for $r \leq \ell$*

$$\begin{aligned}
 \frac{1}{\#\mathcal{C}(A, B)} \sum_{E \in \mathcal{C}(A, B)} \sum_{M_E(N) \geq \ell} M_E(N)^r &= \sum_{m=\ell}^{\ell+\gamma_1} d_{\ell,r}(m) \left(\frac{K(N)N}{\phi(N) \log N} \right)^m + O\left(\frac{N}{\phi(N) \log N}\right)^{1+\ell+\gamma_1} \\
 &\quad + O\left(\frac{1}{(\log N)^{\ell+\gamma_2}}\right),
 \end{aligned}$$

where $\mathcal{C}(A, B)$ is as before.

REMARK 1. Recalling the fact that $d_{\ell,r}(\ell) = \frac{\ell^r}{\ell!}$, we note that Theorem 2 is somewhat similar to the prime ℓ -tuple conjecture except for an extra $\frac{1}{\ell!}$, which comes from the permutation of a ℓ -tuple. Also in Theorem 2 and Theorem 3, the parameter γ_1 is introduced to express the smaller order terms with precise constants. Further in Theorem 3, the implied constant in the last error term is independent of γ_2 .

In the next section we shall define the required notations and prove results that will be useful the proof of the theorems.

2. Some results on estimation of class numbers

Let D be a negative discriminant. Using the class number formula [p. 515, [IK04]], the *Kronecker class number* for a discriminant D can be written as

$$H(D) := \sum_{\substack{f^2 | D \\ D/f^2 \equiv 0,1 \pmod{4}}} \frac{\sqrt{|D|}}{2\pi f} L(1, \chi_{D/f^2}) \quad (2.1)$$

where χ_d is the Kronecker symbol $(\frac{d}{\cdot})$ and $L(s, \chi_d) := \sum_{n=1}^{\infty} \frac{\chi_d(n)}{n^s}$.

Also let

$$D_N(p) := (p+1-N)^2 - 4p = (N+1-p)^2 - 4N, \quad (2.2)$$

Now, for $f^2 \mid D_N(p)$, for $d_{N,f}(p) := \frac{D_N(p)}{f^2}$.

Further, using Deuring's theorem[Deu41] we get

$$H(D_N(p)) = \sum_{\substack{\tilde{E}/\mathbb{F}_p \\ |\tilde{E}(\mathbb{F}_p)|=N}} \frac{1}{\#\text{Aut}(\tilde{E})}, \quad (2.3)$$

where the sum is over the F_p -isomorphism classes of elliptic curves.

With these notations, we have the proposition as follows.

PROPOSITION 1. Fix $R > 0$, for $x \geq 1$, we have that

$$\frac{1}{x} \sum_{1 \leq N \leq x} \left| \sum_{N^- < p < N^+} H(D_N(p)) - \frac{K(N)N^2}{\phi(N) \log N} \right| \ll_R \frac{x}{(\log x)^R}.$$

The above proposition has been proved in (Theorem 1.8, [CDKS15]).

Note that, in our case the $p \approx N$ and $|D_N(p)| \leq 4N$. With these notations, we state the following lemma

LEMMA 1. Let N be a positive integers and N^- and N^+ are defined as in (1.2). Also let $H(D_N(p))$ be defined using (2.1) and (2.2). Then

(a)

$$\sum_{N^- < p < N^+} H(D_N(p)) \ll \frac{N^2}{\phi(N) \log N}.$$

(b) Also for $k \geq 2$,

$$\sum_{N^- < p < N^+} H(D_N(p))^k \ll N^{\frac{k+1}{2}} (\log N)^{k-2} (\log \log N)^k.$$

Proof. Part (a) essentially follows from [Theorem 1.7, [CDKS15]]. Also see [DS13].

For part (b), We recall that

$$H(D_N(p)) = \sum_{\substack{f^2 | D_N(p) \\ \frac{D_N(p)}{f^2} \equiv 0,1 \pmod{4}}} \frac{\sqrt{|D_N(p)|}}{2\pi f} L(1, \chi_{d_{N,f}(p)}).$$

Now $|D_N(p)| \leq 4N$ in the above range of p . Also $L(1, \chi_{d_{N,f}(p)}) \ll \log N$ using convexity bound. Further using the fact that $\sum_{d|n} \frac{1}{d} \ll \log \log n$, we get

$$\begin{aligned} H(D_N(p)) &\ll \sum_{\substack{f^2 | D_N(p) \\ \frac{D_N(p)}{f^2} \equiv 0,1 \pmod{4}}} \frac{\sqrt{N} \log N}{f} \\ &\ll \sqrt{N} \log N \log \log N. \end{aligned} \tag{2.4}$$

Then, (2.4) along with part (a) completes the proof. \square

Probably a stronger bound for the second part of the previous lemma could be proved in Lemma 1(b). But for the purpose of this paper, this result is sufficient.

Now, we recall the following lemma [Corollary 2F, [Sch76]]:

LEMMA 2. *Suppose p is a prime. Suppose $g(x) = a_n x^n + \cdots + a_0$ is a polynomial with integer coefficients having $0 < n < p$ and $p \nmid a_n$. Then*

$$\left| \sum_{x=0}^{p-1} e\left(\frac{g(x)}{p}\right) \right| \leq (n-1)p^{\frac{1}{2}}.$$

3. Curves with fixed order modulo primes

From now on $E_{s,t}$ will denote the elliptic curve given by a Weierstrass equation of the form $y^2 = x^3 + sx + t$. Also if the corresponding field is of characteristic different from 2 or 3, then any isomorphism class of curve can be represented by one such Weierstrass equation. With these notation we state the following result

PROPOSITION 2. *Let $\{p_i\}_{i=1}^\ell$ be a set of ℓ distinct primes in the range $[N^-, N^+]$ and $\{\tilde{E}_{s_i, t_i}/\mathbb{F}_{p_i}\}_{i=1}^\ell$ be a set of isomorphism class of elliptic curves over corresponding fields \mathbb{F}_{p_i} 's. Then for the class of rational curves $\mathcal{C}(A, B)$ as defined in (1.5),*

$$\#\{E \in \mathcal{C}(A, B) : E_{p_i} \cong_{p_i} \tilde{E}_{s_i, t_i} \text{ for } 1 \leq i \leq \ell\} = \frac{4AB}{p_1 \cdots p_\ell} \prod_{i=1}^\ell \left(\frac{1}{|Aut_{p_i}(E_{s_i, t_i})|} \right) + \mathcal{E}_\ell(A, B, N) \tag{3.1}$$

where

$$\mathcal{E}_\ell(A, B, N) \ll \frac{AB}{N^{2\ell}} + N^{\frac{\ell}{2}} (\log N)^2 + (A \prod_{t_i=0} \sqrt{N} + B \prod_{s_i=0} \sqrt{N}) N^{-\frac{\ell}{2}} \log N.$$

Proof. We use a modified version of the character sum argument used by Fouvry and Murty (p. 94, [FM96]). First subdivide the interval $[-A, A]$ into intervals of length $p_1 \cdots p_\ell$, starting from $[-A, -A + p_1 p_2 \cdots p_\ell]$. The last one is denoted by \mathcal{A} . Similarly for $[-B, B]$, with the last one as \mathcal{B} . Using the Chinese remainder theorem, we get

$$\begin{aligned}
 & \#\{E \in \mathcal{C}(A, B) : E \cong_{p_i} \tilde{E}_{s_i, t_i} \text{ for } 1 \leq i \leq \ell\} \\
 &= \left[\frac{2A}{p_1 \cdots p_\ell} \right] \left[\frac{2B}{p_1 \cdots p_\ell} \right] \prod_{i=1}^{\ell} \left(\frac{p_i - 1}{|Aut_{p_i}(E_{s_i, t_i})|} \right) \\
 &+ \left[\frac{2A}{p_1 \cdots p_\ell} \right] \prod_{i=1}^{\ell} \frac{1}{|Aut_{p_i}(E_{s_i, t_i})|} \# \{(u_1, \dots, u_\ell) \in \mathbb{F}_{p_1} \times \cdots \times \mathbb{F}_{p_\ell} : t_i u_i^6 \in \mathcal{B}(\text{mod } p_i) \forall 1 \leq i \leq \ell\} \\
 &+ \left[\frac{2B}{p_1 \cdots p_\ell} \right] \prod_{i=1}^{\ell} \frac{1}{|Aut_{p_i}(E_{s_i, t_i})|} \# \{(u_1, \dots, u_\ell) \in \mathbb{F}_{p_1} \times \cdots \times \mathbb{F}_{p_\ell} : s_i u_i^4 \in \mathcal{A}(\text{mod } p_i) \forall 1 \leq i \leq \ell\} \\
 &+ \prod_{i=1}^{\ell} \frac{1}{|Aut_{p_i}(E_{s_i, t_i})|} \# \{(u_1, \dots, u_\ell) \in \mathbb{F}_{p_1} \times \cdots \times \mathbb{F}_{p_\ell} : s_i u_i^4 \in \mathcal{A}(\text{mod } p_i), t_i u_i^6 \in \mathcal{B}(\text{mod } p_i) \forall 1 \leq i \leq \ell\} \\
 &+ O\left(\frac{AB}{p_1 \cdots p_\ell} \left(\sum_{i=1}^{\ell} \frac{1}{p_i^9}\right)\right), \tag{3.2}
 \end{aligned}$$

where the last error term comes from the rational curves of the form $E_{s_i u_i^4 p_i^4, t_i u_i^6 p_i^6}$.

Now from the fourth term on the right hand side of (3.2),

$$\begin{aligned}
 & \# \{(u_1, \dots, u_\ell) \in \mathbb{F}_{p_1} \times \cdots \times \mathbb{F}_{p_\ell} : s_i u_i^4 \in \mathcal{A}(\text{mod } p_i), t_i u_i^6 \in \mathcal{B}(\text{mod } p_i) \forall 1 \leq i \leq \ell\} \\
 &= \frac{1}{(p_1 \cdots p_\ell)^2} \sum_{\substack{(h_1, \dots, h_\ell) \\ 0 \leq h_i \leq p_i}} \sum_{\substack{(g_1, \dots, g_\ell) \\ 0 \leq g_i \leq p_i}} \sum_{\substack{(u_1, \dots, u_\ell) \\ 1 \leq u_i \leq p_i - 1}} \sum_{(a, b) \in \mathcal{A} \times \mathcal{B}} e \left(\sum_{i=1}^{\ell} \frac{h_i(s_i u_i^4 - a) + g_i(t_i u_i^6 - b)}{p_i} \right), \tag{3.3}
 \end{aligned}$$

where $e(x) = e^{2\pi i x}$.

When $(h_1, \dots, h_\ell) = (0, \dots, 0)$ and $(g_1, \dots, g_\ell) = (0, \dots, 0)$, the R.H.S of (3.3) gives a contribution equal to $|\mathcal{A}||\mathcal{B}| \prod_{i=1}^{\ell} \left(\frac{p_i - 1}{p_i^2}\right)$. Using the fact that \mathcal{A} and \mathcal{B} are intervals, the contributions corresponding to $(h_1, \dots, h_\ell) \neq (0, \dots, 0)$, $(g_1, \dots, g_\ell) \neq (0, \dots, 0)$ is bounded by

$$\begin{aligned}
 & \frac{1}{(p_1 \cdots p_\ell)^2} \sum_{\substack{(h_1, \dots, h_\ell) \neq (0, \dots, 0) \\ 0 \leq h_i \leq p_i - i}} \sum_{\substack{(g_1, \dots, g_\ell) \neq (0, \dots, 0) \\ 0 \leq g_i \leq p_i - 1}} \left\| \frac{h_1}{p_1} + \cdots + \frac{h_\ell}{p_\ell} \right\|^{-1} \left\| \frac{g_1}{p_1} + \cdots + \frac{g_\ell}{p_\ell} \right\|^{-1} \\
 & \times \prod_{i=1}^{\ell} \left(\sum_{u_i=1}^{p_i-1} e \left(\frac{h_i s_i u_i^4 + g_i t_i u_i^6}{p_i} \right) \right). \tag{3.4}
 \end{aligned}$$

If $h_i g_i$ is different from 0 for all i , then $\sum_{u_i=1}^{p_i-1} e \left(\frac{h_i s_i u_i^4 + g_i t_i u_i^6}{p_i} \right) \leq 5\sqrt{p_i}$, using Lemma 2. While if $h_{i_1}, h_{i_2}, \dots, h_{i_r}$ are zero and other h_i are non zero, then

$$\frac{1}{(p_1 \cdots p_\ell)} \sum_{\substack{(h_1, \dots, h_\ell) \neq (0, \dots, 0) \\ 0 \leq h_i \leq p_i - i \\ h_{i_1} = h_{i_2} = \cdots = h_{i_r} = 0}} \left\| \frac{h_1}{p_1} + \cdots + \frac{h_\ell}{p_\ell} \right\|^{-1} = O \left(\frac{\log \left(\frac{p_1 \cdots p_\ell}{p_{i_1} \cdots p_{i_r}} \right)}{p_{i_1} \cdots p_{i_r}} \right).$$

Similar result holds for g_i 's.

Without loss of generality we may assume that $p_i \gg 2^{2\ell}$. In that case (3.4) is

$$O(\sqrt{p_1 \cdots p_\ell} \log(p_1 \cdots p_\ell)^2).$$

Similarly, considering contributions corresponding to $(h_1, \dots, h_\ell) = (0, \dots, 0)$, $(g_1, \dots, g_\ell) \neq (0, \dots, 0)$, as well as $(h_1, \dots, h_\ell) \neq (0, \dots, 0)$, $(g_1, \dots, g_\ell) = (0, \dots, 0)$, (3.3) equals to

$$\begin{aligned} |\mathcal{A}||\mathcal{B}| \prod_{i=1}^{\ell} \left(\frac{p_i - 1}{p_i^2} \right) + O\left(\frac{|\mathcal{A}|}{(p_1 \cdots p_\ell)} \log(p_1 \cdots p_\ell) \prod_{t_i=0} (p_i) \prod_{t_i \neq 0} \sqrt{p_i} \right) \\ + O\left(\frac{|\mathcal{B}|}{(p_1 \cdots p_\ell)} \log(p_1 \cdots p_\ell) \prod_{s_i=0} (p_i) \prod_{s_i \neq 0} \sqrt{p_i} \right) + O(\sqrt{p_1 \cdots p_\ell} \log(p_1 \cdots p_\ell)^2) \end{aligned} \quad (3.5)$$

Proceeding in a similar way for the second and third term in the right hand side of (3.2), we get the following

$$\begin{aligned} \#\{E \in \mathcal{C}(A, B) : E \cong_{p_i} \tilde{E}_{s_i, t_i} \text{ for } 1 \leq i \leq \ell\} &= \left[\frac{2A}{p_1 \cdots p_\ell} \right] \left[\frac{2B}{p_1 \cdots p_\ell} \right] \prod_{i=1}^{\ell} \left(\frac{p_i - 1}{|\text{Aut}_{p_i}(E_{s_i, t_i})|} \right) \\ &+ \left[\frac{2A}{p_1 \cdots p_\ell} \right] \prod_{i=1}^{\ell} \frac{1}{|\text{Aut}_{p_i}(E_{s_i, t_i})|} \left[|\mathcal{B}| \prod_{i=1}^{\ell} \frac{p_i - 1}{p_i} + O\left(\left(\prod_{s_i=0} p_i \right) \left(\prod_{s_i \neq 0} \sqrt{p_i} \right) \log(p_1 \cdots p_\ell) \right) \right] \\ &+ \left[\frac{2B}{p_1 \cdots p_\ell} \right] \prod_{i=1}^{\ell} \frac{1}{|\text{Aut}_{p_i}(E_{s_i, t_i})|} \left[|\mathcal{A}| \prod_{i=1}^{\ell} \frac{p_i - 1}{p_i} + O\left(\left(\prod_{t_i=0} p_i \right) \left(\prod_{t_i \neq 0} \sqrt{p_i} \right) \log(p_1 \cdots p_\ell) \right) \right] \\ &+ |\mathcal{A}||\mathcal{B}| \prod_{i=1}^{\ell} \left(\frac{p_i - 1}{p_i^2} \right) + O\left(\frac{|\mathcal{A}|}{(p_1 \cdots p_\ell)} \log(p_1 \cdots p_\ell) \prod_{t_i=0} (p_i) \prod_{t_i \neq 0} \sqrt{p_i} \right) \\ &+ O\left(\frac{|\mathcal{B}|}{(p_1 \cdots p_\ell)} \log(p_1 \cdots p_\ell) \prod_{s_i=0} (p_i) \prod_{s_i \neq 0} \sqrt{p_i} \right) + O(\sqrt{p_1 \cdots p_\ell} \log(p_1 \cdots p_\ell)^2). \end{aligned}$$

By combining the terms together, we get

$$\begin{aligned} \#\{E \in \mathcal{C}(A, B) : E \cong_{p_i} \tilde{E}_{s_i, t_i} \text{ for } 1 \leq i \leq \ell\} &= \frac{4AB}{(p_1 \cdots p_\ell)^2} \prod_{i=1}^{\ell} \left(\frac{p_i - 1}{|\text{Aut}_{p_i}(E_{s_i, t_i})|} \right) \\ &+ O(\sqrt{p_1 \cdots p_\ell} \log(p_1 \cdots p_\ell)^2) + O\left(\frac{A}{(p_1 \cdots p_\ell)} \log(p_1 \cdots p_\ell) \left(\prod_{t_i=0} p_i \right) \left(\prod_{t_i \neq 0} \sqrt{p_i} \right) \right) \\ &+ O\left(\frac{B}{(p_1 \cdots p_\ell)} \log(p_1 \cdots p_\ell) \left(\prod_{s_i=0} p_i \right) \left(\prod_{s_i \neq 0} \sqrt{p_i} \right) \right), \end{aligned} \quad (3.6)$$

and this proves Proposition 2. \square

LEMMA 3. Let $\mathcal{C}(A, B)$ be as above.

(a) If $A, B > N^{\frac{\ell}{2}}(\log N)^{1+\ell+\gamma_2}$ and $AB > N^{\frac{3\ell}{2}}(\log N)^{2+\ell+\gamma_2}$, then

$$\frac{1}{\#\mathcal{C}(A, B)} \sum_{N^- < p_1 \neq \dots \neq p_\ell < N^+} \{E \in \mathcal{C}(A, B) : \#E_{p_1}(\mathbb{F}_{p_1}) = \dots = \#E_{p_\ell}(\mathbb{F}_{p_\ell}) = N\} = \left(\sum_{N^- < p < N^+} \frac{H(D_N(p))}{p} \right)^\ell + O\left(\frac{1}{(\log N)^{\ell+\gamma_2}}\right).$$

(b) For $r \leq \ell$,

$$\frac{1}{\#\mathcal{C}(A, B)} \sum_{N^- < p_1, \dots, p_r < N^+} \sum_{\substack{E \in \mathcal{C}(A, B), M_E(N) \geq \ell+1 \\ E_{p_1}(\mathbb{F}_{p_1}) = \dots = E_{p_r}(\mathbb{F}_{p_r}) = N}} 1 \ll_\ell \left(\frac{H(D_N(p))}{p} \right)^{\ell+1} + \frac{1}{(\log N)^{\ell+\gamma_2}}$$

Proof. Note that

$$\begin{aligned} \#\{E \in \mathcal{C}(A, B) : \#E_{p_1}(\mathbb{F}_{p_1}) = \dots = \#E_{p_\ell}(\mathbb{F}_{p_\ell}) = N\} \\ = \sum_{\substack{\tilde{E}_1/\mathbb{F}_{p_1} \\ \tilde{E}_1(\mathbb{F}_{p_1})=N}} \dots \sum_{\substack{\tilde{E}_\ell/\mathbb{F}_{p_\ell} \\ \tilde{E}_\ell(\mathbb{F}_{p_\ell})=N}} \#\{E \in \mathcal{C} : E_{p_i} \cong_{p_i} \tilde{E}_i \text{ for } 1 \leq i \leq \ell\}. \end{aligned} \quad (3.7)$$

If $N > 7$, then p is different from 2 and 3. Hence every isomorphism class of curve can be represented in a minimal Weierstrass equation, say $E_{s,t} : y^2 = x^3 + sx + t$ with $s, t \in \mathbb{F}_p$. Let each of the E_i are given as E_{s_i, t_i} . so we can use Proposition 2 to estimate the summand in the right hand side of (3.7).

Now for a fixed prime p_i , the number of isomorphism class of curves E_{s_i, t_i} with $s_i t_i = 0$ is at most 10. Also recall that $\#\mathcal{C}(A, B) = 4AB + O(A + B)$ and $H(D_N(p_i)) = \sum_{E_{s_i, t_i}/\mathbb{F}_{p_i}} \frac{1}{|Aut_{p_i}(E_{s_i, t_i})|}$.

Thus dividing (3.7) by $\mathcal{C}(A, B)$, the sum in the first part of the lemma equals to

$$\begin{aligned} \Sigma_1 &= \sum_{N^- < p_1 \neq p_2 \neq \dots \neq p_\ell < N^+} \sum_{\substack{\tilde{E}_1/\mathbb{F}_{p_1} \\ \tilde{E}_1(\mathbb{F}_{p_1})=N}} \dots \sum_{\substack{\tilde{E}_\ell/\mathbb{F}_{p_\ell} \\ \tilde{E}_\ell(\mathbb{F}_{p_\ell})=N}} \prod_{i=1}^{\ell} \frac{1}{p_i |Aut_{p_i}(E_{s_i, t_i})|} + \hat{\mathcal{E}}_\ell(A, B, N) \\ &= \sum_{N^- < p_1 \neq p_2 \neq \dots \neq p_\ell < N^+} \left(\prod_{i=1}^{\ell} \frac{H(D_N(p_i))}{p_i} \right) + \hat{\mathcal{E}}_\ell(A, B, N) \end{aligned} \quad (3.8)$$

with

$$\hat{\mathcal{E}}_\ell(A, B, N) \ll \left\{ \frac{1}{N^{2\ell}} + \frac{\log N}{N^{\frac{\ell}{2}}} \left(\frac{1}{A} + \frac{1}{B} \right) + \frac{N^{\frac{\ell}{2}}(\log N)^2}{AB} \right\} \left(\frac{N \log \log N}{\log N} \right)^\ell$$

where the implied constant depends on ℓ only. Also since $A, B > N^{\frac{\ell}{2}}(\log N)^{1+\ell+\gamma_2}$, and $AB > N^{\frac{3\ell}{2}}(\log N)^{2+\ell+\gamma_2}$ it follows that

$$\hat{\mathcal{E}}_\ell(A, B, N) \ll \frac{1}{(\log N)^{\ell+\gamma_2}}.$$

Further if we relax the condition $p_1 \neq p_2 \neq \dots \neq p_\ell$ from the right hand side of (3.8), then one gets

$$\begin{aligned}
 \Sigma_1 &= \sum_{\substack{(p_1, p_2, \dots, p_\ell) \\ N^- < p_i < N^+ \ \forall i}} \prod_i \frac{H(D_N(p_i))}{p_i} + \sum_{\substack{(p_1, p_2, \dots, p_\ell) \\ p_i = p_j \text{ for some } i \neq j \\ N^- < p_i < N^+ \ \forall i}} \prod_i \frac{H(D_N(p_i))}{p_i} + O\left(\frac{1}{(\log N)^{\ell+\gamma_2}}\right) \\
 &= \left(\sum_{N^- < p < N^+} \frac{H(D_N(p))}{p} \right)^\ell + O\left(\sum_{r=2}^{\ell} \left(\sum_{N^- < p < N^+} \frac{H(D_N(p))}{p} \right)^{\ell-r} \sum_{N^- < p < N^+} \frac{H(D_N(p))^r}{p^r} \right) \\
 &\quad + O\left(\frac{1}{(\log N)^{\ell+\gamma_2}}\right)
 \end{aligned} \tag{3.9}$$

Using Lemma 1 it is easy to see that

$$\sum_{r=2}^{\ell} \left(\sum_{N^- < p < N^+} \frac{H(D_N(p))^r}{p^r} \right) \left(\sum_{N^- < p < N^+} \frac{H(D_N(p))}{p} \right)^{\ell-r} \ll O(N^{-\frac{1}{2}+\epsilon})$$

for any small $\epsilon > 0$. Hence

$$\Sigma_1 = \left(\sum_{N^- < p < N^+} \frac{H(D_N(p))}{p} \right)^\ell + O\left(\frac{1}{(\log N)^{\ell+\gamma_2}}\right). \tag{3.10}$$

This proves the result part (a) of the Lemma.

Now, if for a curve E , $M_E(N) = L \geq l+1$, then E is counted L^r times in part (b). While the same E will be counted $\frac{L!}{(L-\ell-1)!}$ times if we consider the expression

$$\frac{1}{\#\mathcal{C}(A, B)} \sum_{N^- < p_1 \neq \dots \neq p_{\ell+1} < N^+} \{E \in \mathcal{C}(A, B) : \#E_{p_1}(\mathbb{F}_{p_1}) = \dots = \#E_{p_{\ell+1}}(\mathbb{F}_{p_{\ell+1}}) = N\}$$

Using Stirling's approximation, is easy to see that $\frac{L^r(L-\ell-1)!}{L!} \ll e^\ell$ for $r \leq \ell$. Hence part (b) follows from part (a). \square

Using the previous lemma and modifying the proof of part (a) we shall prove an asymptotic of the left hand side of Lemma (3). More precisely we state the following

PROPOSITION 3. *Let $M_E(N)$ and $\mathcal{C}(A, B)$ be defined as above. If $A, B > N^{\frac{\ell+\gamma_1}{2}}(\log N)^{1+\ell+\gamma_2}$ and $AB > N^{\frac{3(\ell+\gamma_1)}{2}}(\log N)^{2+\ell+\gamma_2}$, then for any positive integer $r \leq \ell$,*

$$\begin{aligned}
 \frac{1}{\#\mathcal{C}(A, B)} \sum_{\substack{E \in \mathcal{C}(A, B) \\ M_E(N) \geq \ell}} M_E(N)^r &= \sum_{j=\ell}^{\ell+\gamma_1} d_{\ell, r}(j) \left(\sum_{N^- < p < N^+} \frac{H(D_N(p))}{p} \right)^j \\
 &\quad + O\left(\sum_p \frac{H(D_N(p))}{p} \right)^{\ell+\gamma_1+1} + O\left(\frac{1}{(\log N)^{\ell+\gamma_2}}\right).
 \end{aligned}$$

Proof.

$$\begin{aligned} \frac{1}{\#\mathcal{C}(A, B)} \sum_{\substack{E \in \mathcal{C}(A, B) \\ M_E(N) \geq \ell}} M_E(N)^r &= \frac{1}{\#\mathcal{C}(A, B)} \sum_{\substack{E \in \mathcal{C}(A, B) \\ M_E(N) \geq \ell}} \left(\sum_{\substack{N^- < p < N^+ \\ E_p(\mathbb{F}_p) = N}} 1 \right)^r \\ &= \frac{1}{\#\mathcal{C}(A, B)} \sum_{N^- < p_1, \dots, p_r < N^+} \sum_{\substack{E \in \mathcal{C}(A, B), M_E(N) \geq \ell \\ E_{p_1}(\mathbb{F}_{p_1}) = \dots = E_{p_r}(\mathbb{F}_{p_r}) = N}} 1. \end{aligned}$$

By breaking the sum into two parts we get the following

$$\frac{1}{\#\mathcal{C}(A, B)} \sum_{N^- < p_1, \dots, p_r < N^+} \sum_{j=\ell}^{\ell+\gamma_1} \sum_{M_E(N)=j} 1 + \frac{1}{\#\mathcal{C}(A, B)} \sum_{N^- < p_1, \dots, p_r < N^+} \sum_{M_E(N) \geq \ell+\gamma_1+1} 1 \quad (3.11)$$

where the range of summation is over $E \in \mathcal{C}(A, B)$ with $E_{p_1}(\mathbb{F}_{p_1}) = \dots = E_{p_r}(\mathbb{F}_{p_r}) = N$. Now, by Lemma 3(b), the last sum in the right hand side is bounded by

$$\left(\sum_{N^- < p < N^+} \frac{H(D_N(p))}{p} \right)^{\ell+\gamma_1+1} + O\left(\frac{1}{(\log N)^{\ell+\gamma_2}}\right)$$

Now, we claim that for $r \leq \ell \leq j \leq \ell + \gamma_1$

$$\sum_{N^- < p_1 \neq p_2 \neq \dots \neq p_r < N^+} \sum_{\substack{E \in \mathcal{C}(A, B), M_E(N)=j \\ E_{p_1}(\mathbb{F}_{p_1}) = \dots = E_{p_r}(\mathbb{F}_{p_r}) = N}} 1 = \frac{1}{(j-r)!} \sum_{N^- < p_1 \neq p_2 \neq \dots \neq p_j < N^+} \sum_{\substack{E \in \mathcal{C}(A, B), M_E(N)=j \\ E_{p_1}(\mathbb{F}_{p_1}) = \dots = E_{p_r}(\mathbb{F}_{p_r}) = N}} 1 \quad (3.12)$$

In fact, any curve $E \in \mathcal{C}(A, B)$ with $M_E(N) = j$ is counted $\frac{j!}{(j-r)!}$ times in the left hand side summation, while on the right hand side, the same curve is counted $j!$ times.

(3.13)

Note that we now consider the first term of (3.11), the primes in the range of summations in (3.11) are not distinct. Then recalling the definition of $S(n, m)$, Stirling number of the second kind, which equals to the number of ways of partitioning a set of n elements into m nonempty sets, we get

$$\sum_{N^- < p_1, \dots, p_r < N^+} \sum_{\substack{E \in \mathcal{C}, M_E(N)=j \\ E(\mathbb{F}_{p_1}) = \dots = E(\mathbb{F}_{p_r}) = N}} 1 = \left(\sum_{m=1}^r \frac{S(r, m)}{(j-m)!} \right) \sum_{N^- < p_1 \neq p_2 \neq \dots \neq p_j < N^+} \sum_{\substack{E \in \mathcal{C}(A, B), M_E(N)=j \\ E_{p_1}(\mathbb{F}_{p_1}) = \dots = E_{p_r}(\mathbb{F}_{p_r}) = N}} 1. \quad (3.14)$$

To simplify the constant on the right hand side, we use the fact that $\sum_{m=1}^r \frac{S(r, m)j!}{(j-m)!} = j^r$. See [(4.1.3), p. 60, [Rom84]].

With this

$$\begin{aligned}
 & \sum_{N^- < p_1 \neq p_2 \neq \dots \neq p_j < N^+} \sum_{\substack{E \in \mathcal{C}(A, B), M_E(N) = j \\ E_{p_1}(\mathbb{F}_{p_1}) = \dots = E_{p_r}(\mathbb{F}_{p_r}) = N}} 1 \\
 &= \sum_{N^- < p_1 \neq p_2 \neq \dots \neq p_j < N^+} \sum_{\substack{E \in \mathcal{C}(A, B), M_E(N) \geq j \\ E(\mathbb{F}_{p_1}) = \dots = E(\mathbb{F}_{p_j}) = N}} 1 - \sum_{N^- < p_1 \neq p_2 \neq \dots \neq p_j < N^+} \sum_{\substack{E \in \mathcal{C}(A, B), M_E(N) \geq j+1 \\ E(\mathbb{F}_{p_1}) = \dots = E(\mathbb{F}_{p_j}) = N}} 1 \quad (3.15)
 \end{aligned}$$

Now we denote the left hand side of (3.12) by $\#\mathcal{C}(A, B) \times \omega(r, j)$ and the first term of the right hand side of (3.15) by $\#\mathcal{C}(A, B) \times \Omega(j, j)$. Also we call the left hand side of (3.14) by $\#\mathcal{C}(A, B) \times \Upsilon(r, j)$. Then in view of (3.12) and (3.14), we get the following set of relations

$$\begin{cases} \Upsilon(r, j) = \frac{j^r}{j!} \omega(j, j), \\ \Omega(t, s) = \sum_{n=s}^{\infty} \omega(t, n) \quad \text{for } t \leq s, \\ \omega(t, n) = \frac{1}{(n-t)!} \omega(n, n) \quad \text{for } t \leq n. \end{cases} \quad (3.16)$$

Now by Lemma 3(a),

$$\Omega(j, j) = \left(\sum_{N^- < p < N^+} \frac{H(D_N(p))}{p} \right)^j + O\left(\frac{1}{(\log N)^{j+\gamma_2}}\right),$$

whenever $A, B > N^{\frac{j}{2}}(\log N)^{1+j+\gamma_2}$ and $AB > N^{\frac{3j}{2}}(\log N)^{2+j+\gamma_2}$.

Now, we replace $\sum_{j=\ell}^{\ell+\gamma_1} \Upsilon(r, j)$ by $\sum_{j=\ell}^{\ell+\gamma_1} z_{\ell, r}(j) \Omega(j, j) + O(\Omega(\ell + \gamma_1, \ell + \gamma_1 + 1))$ where $\{z_{\ell, r}(j)\}$ are some constants to be determined using (3.16). Also note that $\Omega(\ell + \gamma_1, \ell + \gamma_1 + 1) \ll \left(\sum_p \frac{H(D_N(p))}{p}\right)^{\ell+\gamma_1} + \frac{1}{(\log N)^{\ell+\gamma_2}}$.

Then (3.11) equals to

$$\sum_{j=\ell}^{\ell+\gamma_1} z_{\ell, r}(j) \left(\sum_{N^- < p < N^+} \frac{H(D_N(p))}{p} \right)^j + O\left(\sum_{N^- < p < N^+} \frac{H(D_N(p))}{p} \right)^{\ell+\gamma_1+1} + O\left(\frac{1}{(\log N)^{\ell+\gamma_2}} \right).$$

Only thing that remains to be shown is that $\{z_{\ell, r}(j)\}_j$ are equals to $\{d_{\ell, r}(j)\}_j$, as defined in (1.11). For that, we prove the following lemma.

□

LEMMA 4. Consider ω, Ω as variables satisfying the identities in (3.16). Then the solution of the equation

$$\sum_{j=\ell}^{\infty} \frac{j^r}{j!} \omega(j, j) = \sum_{j=\ell}^{\infty} z_{\ell, r}(j) \Omega(j, j)$$

in $z_{\ell, r}(j)$ is given by

$$z_{\ell, r}(j) = \sum_{k=\ell}^j \frac{k^r}{k!} \frac{(-1)^{j-k}}{(j-k)!}.$$

Proof. Using the second equation in (3.16), we have

$$\begin{aligned} \sum_{j=\ell}^{\infty} \frac{j^r}{j!} \omega(j, j) &= \sum_{j=\ell}^{\infty} z_{\ell, r}(j) \Omega(j, j) \\ &= \sum_{j=\ell}^{\infty} z_{\ell, r}(j) \sum_{n=j}^{\infty} \omega(j, n). \end{aligned}$$

By changing the order of summation, the right hand side equals to

$$= \sum_{n=\ell}^{\infty} \sum_{\ell \leq j \leq n} z_{\ell, r}(j) \omega(j, n) = \sum_{j=\ell}^{\infty} \sum_{\ell \leq n \leq j} z_{\ell, r}(n) \omega(n, j)$$

But by the last relation in (3.16), this can be written as

$$\sum_{j=\ell}^{\infty} \left(\sum_{\ell \leq n \leq j} \frac{z_{\ell, r}(n)}{(j-n)!} \right) \omega(j, j)$$

Thus, comparing the coefficients of $\omega(j, j)$ from both sides, we get

$$\sum_{\ell \leq n \leq j} \frac{z_{\ell, r}(n)}{(j-n)!} = \frac{j^r}{j!} \quad \text{for } j \geq \ell. \quad (3.17)$$

Since we are only interested in the values of $z_{\ell, r}(n)$ for $\ell \leq n \leq \ell + \gamma_1$, we consider the following matrix equation

$$AZ = J,$$

where A is the $(\ell + \gamma_1 + 1) \times (\ell + \gamma_1 + 1)$ matrix $(a_{mn})_{m, n}$, where

$$a_{mn} = \begin{cases} 0, & \text{if } m < n, \\ \frac{1}{(m-n)!} & \text{if } m \geq n; \end{cases}$$

Also Z and J are the column matrices

$$\begin{bmatrix} z_{\ell, r}(\ell) & z_{\ell, r}(\ell + 1) & \cdots & z_{\ell, r}(\ell + \gamma_1) \end{bmatrix}^T$$

and

$$\begin{bmatrix} \frac{\ell^r}{\ell!} & \frac{(\ell+1)^r}{(\ell+1)!} & \cdots & \frac{(\ell+\gamma_1)^r}{(\ell+\gamma_1)!} \end{bmatrix}^T$$

respectively.

Now it is not difficult to check that A is an invertible matrix with inverse $B = (b_{mn})$, where

$$b_{mn} = (-1)^{m-n} a_{mn}.$$

Finally, using $Z = A^{-1}J = BJ$, we get the desired value of $z_{\ell, r}(j)$'s. This completes the proof of the lemma. □

4. Proof of Theorem 1 and Theorem 3

Putting $\ell = 1$, $r = 1$ and $\gamma_1 = 0$, $\gamma_2 = \gamma$, from Proposition 3 we get,

$$\frac{1}{\#\mathcal{C}(A, B)} \sum_{E \in \mathcal{C}(A, B)} M_E(N) = \sum_{N^- < p < N^+} \frac{H(D_N(p))}{p} + O\left(\left(\sum_{N^- < p < N^+} \frac{H(D_N(p))}{p}\right)^2 + O\left(\frac{1}{(\log N)^{1+\gamma}}\right)\right) \quad (4.1)$$

for appropriate A, B . Then, using (4.1), we replace $\sum_{N^- < p < N^+} \frac{H(D_N(p))}{p}$ in Proposition 3 by $\frac{1}{\#\mathcal{C}(A, B)} \sum_{E \in \mathcal{C}(A, B)} M_E(N)$. We also recall that $d_{\ell, r}(\ell) = \frac{\ell^r}{\ell}$. Now take $\gamma_1 = 0$, $r = 1$ and consider the sum $\frac{1}{\#\mathcal{C}(A, B)} \sum_{\substack{E \in \mathcal{C}(A, B) \\ M_E(N) = \ell}} M_E(N) = \frac{1}{\#\mathcal{C}(A, B)} \sum_{\substack{E \in \mathcal{C}(A, B) \\ M_E(N) = \ell}} \ell$. Then dividing the last equation by ℓ , Theorem 1 follows immediately from the above discussion.

Again, (4.1) together with Proposition 3 and Theorem A completes the proof of Theorem 3.

5. Proof of Theorem 2

First of all note that

$$\begin{aligned} \sum_{N^- < p < N^+} \frac{H(D_N(p))}{p} &= \frac{1}{N} \sum_{N^- < p < N^+} H(D_N(p)) \left(1 + O\left(\frac{1}{\sqrt{N}}\right)\right) \\ &= \frac{1}{N} \sum_{N^- < p < N^+} H(D_N(p)) + \frac{1}{N^{\frac{3}{2}}} \sum_{N^- < p < N^+} |H(D_N(p))| \end{aligned}$$

Now from Lemma 1(a), we get

$$\sum_{N^- < p < N^+} \frac{H(D_N(p))}{p} = \frac{1}{N} \sum_{N^- < p < N^+} H(D_N(p)) + O\left(\frac{\log \log N}{\sqrt{N} \log N}\right)$$

Also

$$\left(\sum_{N^- < p < N^+} \frac{H(D_N(p))}{p}\right)^j = \frac{1}{N^j} \left(\sum_{N^- < p < N^+} H(D_N(p))\right)^j + O\left(\frac{1}{\sqrt{N}}\right)$$

Then

$$\begin{aligned} \sum_{N \leq x} \left(\sum_{N^- < p < N^+} \frac{H(D_N(p))}{p}\right)^j &= \sum_{N \leq x} \frac{1}{N^j} \left(\sum_{N^- < p < N^+} H(D_N(p))\right)^j + O(\sqrt{x}) \\ &= \sum_{N \leq x} \left(\frac{K(N)N}{\phi(N) \log N}\right)^j + \tilde{\mathcal{E}}_1 \end{aligned}$$

To bound the error $\tilde{\mathcal{E}}_1$, note that

$$\tilde{\mathcal{E}}_1 \ll \sum_{N \leq x} \frac{1}{N^j} \left| \left(\sum_{N^- < p < N^+} H(D_N(p)) \right)^j - \left(\frac{K(N)N^2}{\phi(N) \log N} \right)^j \right| + O(\sqrt{x})$$

Using Lemma 1(a), the right hand side is bounded by

$$\begin{aligned} & \sum_{N \leq x} \frac{1}{N^j} \left| \sum_{N^- < p < N^+} H(D_N(p)) - \frac{K(N)N^2}{\phi(N) \log N} \right| \left(\frac{N^2}{\phi(N) \log N} \right)^{j-1} + O(\sqrt{x}) \\ & \ll \frac{1}{x} \sum_{N \leq x} \left| \sum_{N^- < p < N^+} H(D_N(p)) - \frac{K(N)N^2}{\phi(N) \log N} \right| + \sqrt{x} \end{aligned}$$

Using Proposition 1 with $R = 1 + \ell + \gamma_1$, the last summation is

$$\ll_{\ell, \gamma_1} \frac{x}{(\log x)^{1+\ell+\gamma_1}} + \sqrt{x}.$$

Only thing that remains is to estimate the main term, i.e.

$$\sum_{N \leq x} \left(\frac{K(N)N}{\phi(N) \log N} \right)^j$$

for every $\ell \leq j \leq \ell + \gamma_1$. To do this, we write

$$\left(\frac{K(N)N}{\phi(N)} \right)^j = \Theta F(N-1)G(N)$$

where

$$\begin{aligned} \Theta &= \prod_{p>2} \left(1 - \frac{1}{(p-1)^2} \right)^j \\ F(N) &= \prod_{\substack{p|N \\ p>2}} \left(1 - \frac{1}{(p-1)^2} \right)^{-j} \prod_{p|N} \left(1 - \frac{1}{(p-1)^2(p+1)} \right)^j \\ G(N) &= \left(\frac{N}{\phi(N)} \right)^j \prod_{\substack{p|N \\ p>2}} \left(1 - \frac{1}{(p-1)^2} \right)^{-j} \prod_{p|N} \left(1 - \frac{1}{p^{\nu_p(N)}(p-1)} \right)^j \end{aligned}$$

Note that both F and G are multiplicative functions. We use Theorem 1 of [BG15] with $A(n) = B(n) = 1$, and hence $M(x) = x$. Also if we set

$$f(m) = \sum_{d|m} \mu(d) F(m/d) \tag{5.1}$$

and

$$g(m) = \sum_{d|m} \mu(d) G(m/d), \tag{5.2}$$

then f, g are multiplicative functions. So it is enough to compute the values on prime powers. It

is straight forward to check that

$$f(p^t) = \begin{cases} 1, & \text{if } t = 0 \\ \left(1 - \frac{1}{(p-1)^2}\right)^{-j} \left(1 - \frac{1}{(p-1)^2(p+1)}\right)^j - 1, & \text{if } t = 1 \\ 0, & \text{else,} \end{cases}$$

and

$$g(p^t) = \begin{cases} 1, & \text{if } t = 0 \\ \left(\frac{p}{p-1}\right)^j \left(1 - \frac{1}{(p-1)^2}\right)^{-j} \left(1 - \frac{1}{p(p-1)}\right)^j - 1, & \text{if } t = 1 \\ \left(\frac{p}{p-1}\right)^j \left(1 - \frac{1}{(p-1)^2}\right)^{-j} \left[\left(1 - \frac{1}{p^t(p-1)}\right)^j - \left(1 - \frac{1}{p^{t-1}(p-1)}\right)^j\right], & \text{if } t \geq 2, \end{cases}$$

for an odd prime p .

Also

$$f(2^t) = \begin{cases} (2/3)^j - 1, & \text{if } t = 1 \\ 0, & \text{if } t \geq 2, \end{cases}$$

and

$$g(2^t) = \begin{cases} 0, & \text{for } t = 1 \\ 2^j \left[\left(1 - \frac{1}{2^t}\right)^j - \left(1 - \frac{1}{2^{t-1}}\right)^j\right], & \text{if } t \geq 2. \end{cases}$$

Then from (Theorem 1, [BG15]), we know

$$\frac{1}{x} \sum_{N \leq x} \left(\frac{K(N)N}{\phi(N)}\right)^j = \Theta \sum_{N \leq x} F(N-1)G(N) = \Theta \prod_p \left(1 + \sum_{t \geq 1} \frac{f(p^t) + g(p^t)}{p^t}\right) + O\left(\frac{\log x}{x}\right).$$

But the constant in the main term is nothing but the $C(j)$, which has been defined in (1.10). Using partial summation we get

$$\sum_{N \leq x} \left(\frac{K(N)N}{\phi(N) \log N}\right)^j = C(j) \int_2^x \frac{1}{(\log t)^j} dt + O\left(\frac{x}{(\log x)^{R_1}}\right)$$

for any $R_1 > 0$. By choosing $R_1 = 1 + \ell + \gamma_1$ we completes the proof of Theorem 2.

Acknowledgement

The second author would like to thank Chantal David and Dimitris Koukoulopoulos for some fruitful discussions and their suggestions regarding the presentation of this paper.

REFERENCES

- BCD11 A. Balog, A.-C. Cojocaru, and C. David. “Average twin prime conjecture for elliptic curves”, *Amer. J. Math.* **133** (2011), 1179-1229.
- BG15 R. Balasubramanian, S. Giri. “Mean-value of product of shifted multiplicative functions and average number of points on elliptic curves”, *Journal of Number Theory*, **157** (2015), 37-53.
- BPS12 W. D. Banks, F. Pappalardi, I. E. Shparlinski. “On group structures realized by elliptic curves over arbitrary finite fields”, *Exp. Math.* **21** (2012), 11-25.
- CDKS15 V. Chandee, C. David, D. Koukoulopoulos, and E. Smith. “The frequency of elliptic curve groups over prime finite fields” *Canad. J. Math.* **68** (2016), no. 4, 721761.

- DS13 C. David and E. Smith. “Elliptic curves with a given number of points over finite fields”, *Compositio Math.* **149** (2013), 175-203.
- DS14 C. David and E. Smith. “Corrigendum to Elliptic curves with a given number of points over finite fields”, *Compositio Math.* **150** (2014), no. 8, 1347-1348.
- FM96 E. Fouvry and M. R. Murty. “On the distribution of supersingular primes”, *Canad. J. Math.* **48** (1996), 81-104.
- Kow06 E. Kowalski “Analytic problems for elliptic curves”, *J. Ramanujan Math. Soc.* **21** (2006), 19-114.
- MPS14 G. Martin, P. Pollack and E. Smith. “Averages of the number of points on elliptic curves”. *Algebra Number Theory* **8** (2014), no. 4, 813-836.
- Sch76 W. M. Schmidt “Equations over finite fields. An elementary approach”, *Lecture notes in Math.* **536**: Springer Verlag, 1976.
- Rom84 S. Roman “The Umbral Calculus”. New York, Academic Press: 1984, 59-63.
- IK04 H. Iwaniec and E. Kowalski. “Analytic number theory”, colloquium publications, vol. 53, American Mathematical Society, 2004.
- Kou15 D. Koukoulopoulos “Prime numbers in short arithmetic progressions”. *Int. J. Number Theory*, **11** (2015), no. 5, 1499-1521.
- Deu41 M. Deuring “Die Typen der Multiplikatorenringe elliptischer Funktionenkorpr”. *Abh. Math. Sem. Univ. Humbury*, **14** (1941), no. 1, 197-272.

R. Balasubramanian balu@imsc.res.in

Department of Mathematics, Institute of Mathematical Sciences, Chennai, India-600113

Sumit Giri sumit.giri199@gmail.com

School of Mathematics, Tel Aviv University, P.O.B. 39040, Ramat Aviv, Tel Aviv 69978, Israel.